

Appl. No. 10/076,199
Amdt. dated May 21, 2007
Reply to Office Action of March 19, 2007

Amendments to the Claims:

The following will replace all prior versions, and listings, of claims:

Listing of Claims:

1. (Currently Amended): An automated encryption system for encrypting an electronic message from a sender to a recipient comprising:
 - a computer readable medium in communications with a sender's e-mail client;
 - a set of encrypted private keys associated with senders' ID's and passwords stored in said computer readable medium;
 - a set of computer readable encryption instructions embodied in said the computer readable medium for receiving said the electronic message from said the e-mail client that is created by the sender and addressed to the recipient having the sender's ID and password, attempting to decrypt the sender's private key according to said the sender's ID and password, if the sender's private key is successfully decrypted, attempting to retrieve said the recipient's public key from said the computer readable medium, medium; if the sender's private key is successfully decrypted, but and the recipient's public key is not located in said the computer readable medium, attempting to retrieve the recipient's public key from a PKI server in communications with said the computer readable medium if said recipient's public key is located, encrypting said electronic message according to said the recipient's public key, forwarding said the encrypted message to the recipient for subsequent retrieval so that the electronic message is

Appl. No. 10/076,199
Amtd. dated May 21, 2007
Reply to Office Action of March 19, 2007

automatically encrypted and delivered to the recipient without the need for the email client to retrieve the recipient's public key or encrypt the message.

2. (Currently Amended): The system of claim 1 wherein:

 said set of computer readable encryption instructions include instructions for retrieving said the private key associated with the sender from said set of private key data and digitally signing said the electronic message from the sender according to said the private key associated with the sender so that the recipient can verify the authenticity of said the electronic message.

3. (Currently Amended): The system of claim 1 wherein:

 said set of computer readable encryption instructions include instructions that if the sender's private key is successfully decrypted but the recipient's public key is not located on said the PKI server, attempting to retrieve the recipient's public key from a certificate authority in communications with said the computer readable medium.

4-6 (Cancelled)

7. (Currently Amended): They system of claim 1 including:

 a set of computer readable key maintenance instructions embodied within said the computer readable medium for creating a key pair having said at least one public key associated with the sender and a private key associated with said the public key and the sender, storing said the public key within said set of public key data so that said the public key associated with the sender is available for retrieval, receiving a password from the sender, encrypting said the private key according to said the password, storing said the

Appl. No. 10/076,199
Amdt. dated May 21, 2007
Reply to Office Action of March 19, 2007

encrypted private key within said private key data so that the sender can retrieve said the private key for decrypting messages sent to the sender, and, deleting said key pair to prevent the sender from decrypting encrypted messages so that an automated key management system is provided for automatically managing key pairs for senders.

8-19. (Cancelled)